UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	
v.	CRIMINAL NO. 21-cr-10104-PBS
VLADISLAV KLYUSHIN Defendant	(Leave to file granted 1/6/2023)

DEFENDANT VLADISLAV KLYUSHIN'S SUPPLEMENTAL REQUEST TO EXCLUDE GEOLOCATION EVIDENCE

Now comes the defendant Vladislav Klyushin, by and through undersigned counsel, and hereby respectfully submits this supplemental request to exclude the government's IP geolocation analysis from evidence in this case. Failing an expert foundational proffer surviving *Daubert* scrutiny, the analysis is terminally unreliable, and its underlying data defies authentication under Fed R. Evid. 901(a) and (b)(9). The prospective evidence also offends the hearsay rule and violates the Confrontation Clause. Finally, Evidence Rules 401, 802 and 901(a) likewise bar newly proffered "invoices" purporting to show that relevant "computers were, in fact, located in *Boston during th[e] approximate time period*" in question, Dkt. 125 at 25 (emphasis added).

The defense agrees that "[t]he location of [the 104 IPs] is significant to the Court's venue over this prosecution." *Id.* Indeed, the crux of the government's venue allegations is that Mr. Klyushin or his co-conspirators used "servers located in the District of Massachusetts as part of their scheme." *See* Dkt. 1-1 at 8. Notably, though, the Indictment alleges only two instances where Boston, MA servers were used: (1) "On or about October 22, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2," Indictment at ¶ 19; and (2) "On or about October 24, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized

access to the computer network of Filing Agent 2 via another Boston IP address (collectively, the "Boston IP Addresses"), and to view the quarterly financial results of Tesla, Inc. ("Tesla"), the securities of which are publicly traded on the NASDAQ," Indictment at ¶22. Those two allegations form the sole basis for venue in the District of Massachusetts, with the alleged October 24, 2018, intrusion the lone predicate for Counts 2 and 3.

The allegation that the two IP addresses were routed through a data center located in Boston, Massachusetts, in turn, rests on analysis and data from MaxMind, an IP geolocation company that allows users to use "GeoIP data to locate their Internet visitors and show them relevant content and ads, perform analytics, enforce digital rights, and efficiently route Internet traffic." *https://www.maxmind.com/en/company*. As detailed below, however, MaxMind's services are flawed and susceptible to a high risk of error. They are based on data that can't be authenticated and is easily manipulated. And the results they yielded in this case are not corroborated by any records. Even the Micfo invoices the government now proffers[1] fail to corroborate Boston as the server location during the critical time period of October 22 and 24, 2018.

Though it may seem a technicality, this issue is pivotal if not dispositive. It implicates and potentially impugns the sole basis for laying venue in this District — a procedural touchstone enshrined in the Constitution itself — and invoking this Court's territorial jurisdiction. It calls into question, in short, the propriety of trying — and perhaps even extraditing — Mr. Klyushin here.

[1] Having just received these invoices in discovery on December 21 and 22, the defense lacked an opportunity to address their admissibility in its Omnibus Motion *in Limine*.

I. MaxMind Analyses.

The two IP addresses at issue – 104.238.37.190 and 104.238.37.197 – are alleged to have been "hosted at a data center located in Boston, Massachusetts" and used to access "the computer network of Filing Agent 2," Indictment at ¶22. MaxMind's analyses and data assert that these two IP addresses are affiliated with Internet Service Provider (ISP) Web2Objects LLC, a company with locations in Germany and New York, and that at the relevant time,[2] traffic from the addresses was routed through a Boston data center. *See* Exhibit 1. But these analyses and their underlying methodology are deeply flawed.

First, MaxMind itself concedes that "[i]t is not possible [] to guarantee 100% geolocation accuracy." *https://support.maxmind.com/hc/en-us/articles/4407630607131-Geolocation-Accuracy* ("Accuracy exhibits high variability according to country, distance, type of IP (cellular vs. broadband, IPv4 vs. IPv6), and practices of ISPs. We do not guarantee exact matches to our competitors' data, nor identical accuracy to theirs, as we may use different data providers in some instances."). With that caveat, MaxMind estimates – sans independent testing or validation – that its analyses and data are 80% accurate at the state/region level and only *66% accurate at the city level within a 50 km radius of that city*. *Id.* A 50 km (i.e., 31-mile) radius from Boston, however, could potentially put the location of the server in the districts of Rhode Island or New Hampshire.

To make matters worse, MaxMind allows any member of the public – whether the FBI, a lawyer or literally anyone else – to submit modifications to its dataset, making it impossible to know whether the data is based on a reliable source or an unauthenticated, out-of-court statement

[2] Based on counsel's review of MaxMind's offerings and products, it does not provide historical IP geolocation data, *i.e.*, the location of the two IP addresses in October 2018. It only provides IP geolocation data at the time the request is made, *e.g.*, at the time counsel ran the search.

by a third party. *See https://www.maxmind.com/en/geoip-data-correction-request*. Even if MaxMind employees review the underlying correction, their review is not based on any known or reliable scientific principles. Indeed, defense counsel submitted a "correction" to MaxMind in connection with all the IP addresses in the 104.238.37 range requesting that it change the location of the server associated with those addresses from Boston, MA to Lewes, DE. MaxMind's review team approved the change within a matter of hours and changed the data on its public website – switching the relevant servers' location to Lewes, DE – on December 16, 2022. *See* Exhibits 3A-B.

The unreliability of MaxMind's data and analyses is well known and has caused tremendous hardship. *Arnold v. MaxMind, Inc.*, 216 F. Supp. 3d 1275 (D. Kan. 2016) (MaxMind misidentified 600 million IP addresses that had been used for illegal, immoral, or embarrassing purposes with Kansas residence, prompting repeated visits and calls from law enforcement officers, business owners, and private investigators); *see also* Travis M. Andrews, LAWSUIT: HOW A QUIET KANSAS HOME WOUND UP WITH 600 MILLION IP ADDRESSES AND A WORLD OF TROUBLE, THE WASHINGTON POST (2021), https://www.washingtonpost.com/news/morning-mix/wp/2016/08/10/lawsuit-how-a-quiet-kansas-home-wound-up-with-600-million-ip-addresses-and-a-world-of-trouble/ (last visited Dec 13, 2022) ("[MaxMind] maps IP addresses, a notoriously unreliable practice. Many can't be directly linked to an address, only a state or even a country. For its tech to work, MaxMind matched each IP address to a set of coordinates…. [including] mapping [m]ore than 600 million IP addresses [] to [a] yard.").[3] In short, MaxMind's

[3] *See also, e.g.*, *Strike 3 Holdings, LLC v. Doe*, 351 F. Supp. 3d 160, 161-62 (D.D.C. 2018) (Lamberth, J.) ("using geolocation technology to trace" an IP "address to a jurisdiction" is "famously flawed: virtual private networks and onion routing spoof IP addresses (for good and ill); routers and other devices are unsecured; malware cracks passwords and opens backdoors; multiple people (family, roommates, guests, neighbors, etc.) share the same IP address; a

analyses and data are intended to be commercial products utilized by advertisers and companies to track users. They were not intended to be a reliable basis to institute a criminal prosecution resulting in the arrest, extradition, and pretrial confinement of Mr. Klyushin.

Second, MaxMind's analysis clashes with those of other IP geolocation service providers, including some servicing the country's largest technology companies. IP2Location, for example, places the location of the data center with the two operative IP addresses in New York City – hundreds of miles from Boston. *See* Exhibit 4. IPinfo, "the most reliable, accurate, and in-depth source of IP address data available anywhere," see https://ipinfo.io/about, which is used by 500,000+ developers and businesses, including large tech companies like Ebay and Dell, places the location of the server associated with the two IP addresses in Lewes, DE – even farther from Boston. *See* Exhibit 5. Another IP geolocation service used by Amazon, Samsung, and Microsoft, DB-IP, places the location of the server in Chicago, IL – half the country away from this District. *See* Exhibit 6.

Third, the log records of Filing Agent 2 – the only contemporaneous connection records that exist in this case – match IPinfo's results and contradict MaxMind's, also placing the location of the servers associated with these two IP addresses in Lewes, DE. Though FA 2's log

---

geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another") (citing James Temple, *Lawsuit Says Grandma Illegally Downloaded Porn*, S.F. Chron. (July 15, 2011, 4:00 AM), https://www.sfgate.com/business/article/Lawsuit-says-grandma-illegally-downloaded-porn-2354720.php)), *rev'd*, 964 F.3d 1203 (D.C. Cir. 2020); *cf. Strike 3 Holdings, LLC v. Doe*, No. 3:21-cv-993 (MPS), 2021 WL 4776519, at *2 n.2 (D. Conn. Oct. 13, 2021) (noting that courts continue to rely on Judge Lamberth's decision, despite appellate reversal, to impose protective conditions on even preliminary civil jurisdictional discovery) (collecting cases); *Malibu Media, LLC v. John Does 1-13*, No. 2:12–CV–177–FtM–29SPC, 2012 WL 3962492, at *1 (M.D. Fl. Aug. 1, 2012) (deeming *Daubert* considerations premature and declining to engage or address them in preliminary civil jurisdictional discovery context), *report and recommendation adopted*, 2012 WL 3946018 (M.D. Fl. Sep. 10, 2012).

files encompass over 750,000 entries for multiple users and myriad IP addresses, not a single IP address that connected to FA 2's servers originated from the District of Massachusetts according to its own records – including the two IPs in question. *See* Exhibit 7. The Government intends to introduce these records, or portions of them, into evidence as reliable proof of unauthorized intrusions into FA 2's network, but to the extent the Government asserts FA 2's log files are correct and reliable, they also undermine the reliability of MaxMind's analyses.[4]

Fourth, and most important, subpoena responses indicate that the companies associated with the two IP addresses in October 2018 have no record of either – 104.238.37.190 or 104.238.37.197 – being routed through a data center located in Boston at that time. In response to a subpoena, the company that was purportedly assigned the two IP addresses in October 2018 confirmed through counsel that although using them that year, it could not locate any record that either was routed through a Boston server in October. Aside from MaxMind's flawed and easily manipulated data, there is no other evidence that implicates the District of Massachusetts as the location of any alleged conduct during the two relevant dates.

II. Micfo Invoices

The government further intends to introduce "invoices from a now-defunct company called Micfo, which owned the computers on which the 104 IPs resided, and leased space in a data center in Boston to house them." Dkt. 125 at 26. The invoices, however, are irrelevant to whether the IP addresses were associated with servers located in Boston, MA in October 2018. And given Micfo's own fraud conviction, they're patently unreliable. Indeed, the government's filing tellingly leaves out that Micfo, the company that purportedly created and sent these

[4] The Government can't have it both ways – two contradictory pieces of evidence both offered as reliable proof should not be submitted for the jury's consideration.

invoices, itself was indicted and pled "guilty to twenty counts of wire fraud" in connection with fraudulently obtaining and assigning IP addresses through falsified business records. *See* DOJ Press Release, attached hereto as Exhibit 8. That fraud was perpetrated from February 2014 until May 2019, *i.e.*, during the very period when Micfo allegedly hosted the 104 IP addresses in Boston.

Equally problematic, the invoices the government proffers are not relevant to October 2018. The first set of invoices produced to the defense, attached hereto as Exhibit 9, contain unpaid invoices for hosting the data center in Boston from December 1-31, 2018 and December 11, 2018-January 10, 2019. It is unclear why the two unpaid invoices overlap, but both, according to records from the producing entity, Stackpath LLC, show that these invoices are unpaid, and it is uncertain whether those services were ever provided. Exhibit 9 at 7-11. The other invoices from the first batch show paid invoices for hosting nearly a year later – from July-31, 2019 and August 1-31, 2019. Also unclear from this production is why Stackpath LLC – a company that did not acquire Micfo and has no discernible connection to it – is the custodian of Micfo records and should be allowed to testify to their authenticity and how these business records were made and kept.[5]

The second group of invoices, attached hereto as Exhibit 10, come from an entirely unidentified source. The only difference between these invoices and the first set is that they reflect payment to host the IP address in Boston from December 1-31, 2018, December 11, 2018-January 10, 2019 and January 1-30, 2019. Again, it is unclear why all three invoices overlap and who is the custodian of these records.

[5] Despite the defense's request, the government has not identified a relationship between StackPath and Micfo.

III. This Honorable Court should exclude the MaxMind analyses as unreliable.

Though the government would trace the two IP addresses to Boston through MaxMind analysis, its expert disclosures proffer no witness to authenticate or establish the reliability of the data the service uses – conditions precedent to receiving this sort of novel geolocation evidence. Indeed, courts typically require expert testimony demonstrating the accuracy and reliability of similar techniques, refusing to admit their results in its absence. *See, e.g., United States v. Crawford*, No. 19-CR-170-RJA-MJR, 2021 WL 2367592, at *3 (W.D.N.Y. Jan. 14, 2021) ("the Government will need to provide an expert witness to explain and support the methods used by Google to obtain the geolocation data if it intends to use it as evidence at trial"), *report and recommendation adopted*, No. 19-CR-170-A, 2021 WL 1730875 (W.D.N.Y. May 3, 2021); *United States v. Blouin*, No. CR16-307 TSZ, 2017 WL 3485736, at *1, *7 (W.D. Wash. Aug. 15, 2017) (where government deployed "software known as RoundUp eMule" to allegedly link IP addresses to defendant's computer, the program was, "in essence, the witness[] against defendant," so the "dispositive question" was whether it "operates in the manner asserted by the Government and engages in single-source downloading"; court allowed evidence, but only after program developer testified at a pretrial hearing about "how he created the program, what the program is designed to do, and whether, in his opinion, the program does what was intended").

When a party moves to introduce scientific, technical, or specialized expertise this Court must, under Fed. R. Evid. 104(a) and 702, act as a "gatekeeper" to ensure the evidence "is not only relevant, but reliable." *Daubert v. Merrell Dow Pharmaceutical*, 509 U.S. 579, 589 (1993) (emphasis added); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141 (1999) (extending *Daubert*'s holding to expertise deemed "technical" or "specialized knowledge" under Rule 702); *General Electric Co. v. Joiner*, 522 U.S. 137, 142 (1997). Without expert testimony satisfying

Daubert's strictures, nothing indicates – much less establishes – that MaxMind analysis is reliable enough for the Government to parade its results before the jury.

To the contrary, the service itself proclaims that its location data is only 66% reliable at the city level within a 50 km range. This creates the very real potential that the server in question was located outside the District of Massachusetts. *See Digital Sins, Inc. v. John Does 1-245*, No. 11 CIV. 8170 CM, 2012 WL 1744838, at *5 (S.D.N.Y. May 15, 2012) ("there are places in the United States where locations 'within or near the geographic location' of a courthouse are not necessarily in the same district, or even the same state, as that courthouse"). Owing to these accuracy limitations, MaxMind's analyses have, in certain instances, been held insufficient to establish even preliminary jurisdiction in civil cases. *See Strike 3 Holdings, LLC v. Doe*, No. 18CV231-BEN (BLM), 2018 WL 1071711, at *2 (S.D. Cal. Feb. 23, 2018) (Maxmind analysis was insufficient "to show that Defendant's IP address likely resolves to a physical address located in this District, and this Court cannot rely on Plaintiff's unsupported assertions regarding the use and accuracy of the geolocation technology Plaintiff contends to have applied."). Here, MaxMind's reliability is further undercut by several stark facts: (1) other IP geolocation services are not in consensus as to the location of the two IP addresses, (2) FA 2's own logs report connections from Lewes, DE rather than Boston, MA on the dates in question and (3) the owners and users of the two IP addresses have no records corroborating MaxMind's assertion that they originated from a Boston server.

What's more, the method by which MaxMind accumulates and verifies data – *i.e.*, the fact that anyone can ask MaxMind to alter its dataset and such requests are approved without any rigor – not only evinces a lack of reliability, but also implicates Fed. R. Evid. 901(a) and (b)(9), the rule against hearsay, and the confrontation clause. Rule 901(a) requires "the proponent [to]

produce evidence sufficient to support a finding that the item is what the proponent claims it is." To present trial evidence emanating from "a process or system," the proponent must make a threshold showing "that it produces an accurate result." Fed R. Evid 901(b)(9). *See Crawford*, 2021 WL 1730875, at *2 ("Whether the Google cell phone location data, or a map derived from it, is admissible during the trial will depend on whether the requirements of Fed. R. Evid. 901(a) are satisfied by a showing that the location data is what it purports to be."). Properly applied here, then, Rule 901 requires the Government to demonstrate preliminarily that the way MaxMind receives, reviews, and publishes data produces results that are sound and accurate.

Accuracy considerations aside, the fact that MaxMind accepts data corrections from any individual also creates hearsay and confrontation problems. After all, anyone – regardless of whether the statement is true or satisfies a hearsay exception (*e.g.*, business records) – can edit, supplement or correct MaxMind's data, as evidenced by counsels' correction to the data associated with the relevant IP addresses. MaxMind's analysis incorporates that hearsay without identifying the information's underlying source, preventing cross-examination of the proffering party and violating the Confrontation Clause. One of MaxMind's intended purposes is to help "enforce digital rights," *i.e.*, to allow litigants access to geolocation data to prosecute patent and copyright infringement lawsuits. These are textbook "'statements … made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial.'" *Crawford v. Wash.*, 541 U.S. 36, 52 (2004) (*quoting* Brief for National Association of Criminal Defense Lawyers *et al. as Amici Curiae* 3, 2003 WL 21754961).

Finally, the government's citation to Fed. R. Evid. 803(17) is unavailing. That hearsay exception is intended for "[m]arket quotations, lists, directories, or other compilations that are

generally relied on by the public or by person in particular occupations," *e.g.*, telephone directories and the stock listings. Conversely, the government fails to cite a single reported criminal case that relies on MaxMind as the basis for locating the servers of a specific IP address. *See Crane v. Crest Tankers, Inc.*, 47 F.3d 292, 2961 (8th Cir. 1995) (holding it reversible error to admit a "Future Damage Calculator": "[a]ppellee … made no showing and offered no foundation that the exhibit is generally used or relied upon by the public or persons in the legal or other professions"). Indeed, even in the civil context, as cited above, courts have found largely unchallenged, *ex parte* MaxMind proffers only *prima facie* reliable enough to permit preliminary jurisdictional discovery. At the same time, many voice serious concerns about the service's accuracy and some reject its results altogether, while otherwise deeming *Daubert* claims premature in that posture. In *criminal* prosecutions, by contrast, courts usually demand an expert reliability showing before admitting geolocation evidence at trial. Because the government spurns that prerequisite here, exclusion must follow.

IV. This Honorable Court should exclude the Micfo invoices.

Far from corroborating the MaxMind information as the government fancies, its newly proffered Micfo invoices stir more questions than answers and should also be excluded from evidence. First, they are irrelevant.[6] None of the invoices relate to the October 2018 period when the alleged intrusions into Filing Agent 2 took place. It is impossible to predict the location of a server or IP address in October 2018 based on its alleged location in December 2018, January

[6] *See, e.g., Criminal Productions, Inc. v. Doe-72.192.163.220*, No. 16-cv-2589 WQH (JLB), 2016 WL 6822186, at *2 (C.D. Cal. Nov. 18, 2016) (because a person using a dynamic IP address "one month may not have been the same person using it the next," geolocation efforts are "irrelevant" unless performed in "temporal proximity" to offending conduct) (citation and internal quotation marks omitted).

2019, July 2019, or August 2019. IP addresses are typically portable.[7] Meaning that you can move an IP address and associate it with different data centers on a whim. It is akin to moving a telephone number from one provider to another. *Strike 3 Holdings, LLC v. Doe*, 2019 WL 5446239, at *11 (D.N.J. Oct. 24, 2019) ("due to dynamic IP addresses the name of the subscriber identified by Strike 3's November 13, 2018 subpoena may not be the person who subscribed to the same address on July 27, 2018. This information is not revealed by Strike 3 even though Strike 3 recognizes there are a limited number of IP addresses, the addresses are dynamic, and they therefore change."). Accordingly, for an invoice to be relevant it must encompass October 2018.

Second, Micfo is a company that has been convicted of fraudulently obtaining and assigning IP addresses through falsified businesses and records. Confounding logic, the government now proffers Micfo invoices as reliable business records when it just recently prosecuted the same company for fraud in connection with its business model during the same relevant period.

Third, the government has not proffered a witness who could authenticate the invoices under Fed R. Evid. 901(a) or satisfy the requirements of Fed R. Evid. 803(6). StackPath LLC, the purported record keeper for Micfo invoices, has, to counsel's knowledge, no connection to the company. It can't testify as to how the invoices were made or kept.

In sum, the burden is on the government to prove not only authenticity, but also the invoices' admissibility under Rule 803(6). Micfo's prior fraud conviction should foreclose their

[7] *Ibid.* & nn. 1-2 (explaining that "Dynamic IP addresses," the most common form, are "randomly assigned to internet users and change frequently. Consequently, for dynamic IP addresses, a single IP address may be re-assigned to many different computers in a short period of time.") (citations and internal quotation marks omitted).

admissibility as reliable business records. *See* Fed. R. Evid. 803(6)(E) ("A record of an act, event, condition, opinion, or diagnosis [is not hearsay] if …. [] the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness."). Accordingly, this Honorable Court should also exclude the Micfo invoices from evidence.

Respectfully Submitted,

Vladislav Klyushin,
By His Attorney,

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.
Mass. Bar No. 690826
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
menemtsev@gmail.com

/s/ Marc Fernich
Marc Fernich
Law Office of Marc Fernich
800 Third Avenue
Floor 20
New York, NY 10022
212-446-2346
Email: maf@fernichlaw.com

Dated: January 9, 2023

CERTIFICATE OF SERVICE

I, Maksim Nemtsev, hereby certify that on this date, January 9, 2023, a copy of the foregoing documents has been served via Electronic Court Filing system on all registered participants.

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.